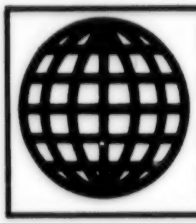
JPRS-CST-89-022
10 OCTOBER 1989



FOREIGN
BROADCAST
INFORMATION
SERVICE

JPRS Report

China

SCIENCE AND TECHNOLOGY
Computer Viruses

Science & Technology

CHINA

Computer Viruses

JPRS-CST-89-022 *10 October 1989*

CONTENTS

Prevention, Cure of Computer Viruses *[Xiong Zhang; JISUANJI SHIJIE, 19 Jul 89]* 1
The Most Common Computer Viruses *[JISUANJI SHIJIE, 19 Jul 89]* 2
Overview of Computer Viruses *[Chen Yousong; JISUANJI SHIJIE, 19 Jul 89]* 5
Virus Attacks on Computers *[Li Juyi; JISUANJI SHIJIE, 19 Jul 89]* 7
Method Described for Detecting a Shell Virus *[Xi Hongyu; JISUANJI SHIJIE, 19 Jul 89]* 9
New Virus and Anti-Viral Measures Described *[JISUANJI SHIJIE, 19 Jul 89]* 10
Discovery of Another Chinese Virus, Appropriate Measures *[Yu Dong; JISUANJI SHIJIE, 19 Jul 89]* 11
One Way To Disinfect a Computer Virus *[Zhang Yingqi; JISUANJI SHIJIE, 19 Jul 89]* 13
Program Listing for Detoxifying, Vaccinating Disks *[Jiang Mingfu; JISUANJI SHIJIE, 19 Jul 89]* 15
Another Method for Disinfecting Computer Disks *[Gao Guoming; JISUANJI SHIJIE, 19 Jul 89]* 15
Analysis of an Operating System Virus, Prevention and Cure
[Xi Hongyu; JISUANJI SHIJIE, 19 Jul 89] 16

Prevention, Cure of Computer Viruses

40080222a Beijing JISUANJI SHIJIE [CHINA COMPUTERWORLD] in Chinese No 28, 19 Jul 89 p 33

[Article by Xiong Zhang [3574 3864], visiting scholar in the United States from the Computer Department of Beijing Aerospace University: "Computer Viruses and Their Prevention and Cure"]

[Text] Editor's note: Since computer viruses were first discovered in the United States, many countries and regions throughout the world (including China) have uncovered invasions by computer viruses. In their mortal attacks on computers, computer viruses have already stolen large amounts of manpower and financial resources from computer users. "Viruses" have become assailants the very name of which makes all computer users shudder.

Current varieties of viruses are continuing to multiply, and many practical jokers are intent upon giving full rein to their "extraordinary intellects." Because of this, those working on computer security have come up with several effective "vaccines" for preventing viruses, and software that detects and diagnoses computer viruses and repairs [damage] is continuing to appear. But both vaccines and restorative software are directed at the types of viruses that have been discovered so far, and as of this moment, there is no all-purpose vaccine that will allow computer users to sit back and relax, that can render a computer immune for all its life. What are computer viruses, anyway? Are they as fearsome as everyone says? Are there any more effective preventative measures? These questions have attracted the widespread concern of our readers, for which reason this newspaper has arranged for the writing of several articles about computer viruses, which we are publishing as a special issue. [End of editor's note]

The computer virus, once considered science fiction, has quite genuinely appeared before everyone's eyes and has become a serious threat.

The Computer Virus

A computer virus is a computer program, which differs from other programs in being able to propagate and be transmitted like a biological virus. What is more, it constitutes a danger to computer systems and makes off with large quantities of funds, manpower, and computer resources. This kind of danger may not be taken lightly, for according to incomplete statistics, approximately 90,000 computers in the United States were infected with viruses during 1988, while in November of that year alone virus infections generated losses in excess of US$100 million. One regularly hears reports of viruses invading computer systems in other countries, too.

The varieties of virus that have been discovered so far have increased from the seven of February 1988 to more than 30 at present. Different viruses have different symptoms. The smaller ones have only 20 instructions in fewer than 50 bytes, while larger ones are like an operating system and consist of tens of thousands of instructions. Some are transmitted quickly, and can crash a system as soon as they invade it. Others have a longer dormancy, only becoming active 2 or 3 years after infection. Some viruses infect all programs and data in a system, while others are only interested in certain kinds of programs or data. Most viruses do not crash the entire system in the beginning, but rather move the decimal points in a database or other data file a little to the left or right, adding or subtracting 1 or 2 zeros. Some viruses do nothing more than copy themselves repeatedly, touching nothing, and certainly this kind of danger is not as reprehensible as that of crashing entire systems.

The majority of viruses discovered by now are spreading through IBM PCs and their compatibles, and so viruses are an important threat to computer circles in China.

The Spread of Computer Viruses

The ability to spread is considered a major characteristic of viruses. There are generally three means by which viruses enter a system:

1. By use of a floppy disk that has been infected elsewhere. When a user buys a computer, he might bring his own disk to test the machine; people promoting software might demonstrate their software on a user's computer. These are both ways in which a virus is transmitted.

2. By moving an infected computer. An infected computer being moved from one office to another can take along a virus.

3. By electronic communications. Communications via computer networks, and especially through the exchange of executable code, is a very easy way to transmit viruses.

The Prevention and Cure of Computer Viruses

Obviously, it is more important to prevent viruses from entering than to discover and eradicate them after they invade. Seeing how viruses are transmitted, the best method for preventing virus invasions is to block these means of transmission.

1. The first thing to be careful of is the use of public and shared software, because the people who use this kind of software are many and diverse, which increases the likelihood that the software carries a virus.

2. Second, software from outside the office should not be used by any means, even if some disks have only been taken home by office personnel, because who can guarantee that their computers have not been infected?

3. Only use a computer that has been recently moved into the office after it [i.e., the computer] has been "disinfected";

4. Restrict the network exchange of executable code;

5. Write-protect all system disks and software;

6. Use only original disks, and by no means use a floppy disk to boot a hard disk;

7. Never run programs having unknown origins;

8. Never write user data or programs onto a system disk.

The measures just listed are effective means by which to prevent the invasion of viruses.

If you cannot prevent the introduction of viruses, then you should discover their presence as soon as possible. Obviously, the earlier a virus is discovered the better, and if you can discover and eradicate it before it causes damage, then you will have prevented damage to the system; if you can discover it before it has spread widely, then you can lighten and ease the burden of restoring the system. All in all, the longer a virus resides in a system, the greater the damage it will cause.

A virus must be transmitted by copying itself, and copying takes time, so the existence of a virus might be discovered by an increase in the execution time of a program or by taking longer to write onto a disk. These things are certain to leave clues, and a trained and alert user might discover a virus in this way. Keeping the following situations in mind can help a user discover a virus as soon as possible:

1. A program takes longer to load than normal;

2. Disk access time is longer than normal;

3. Unusual information appears in a consistent manner;

4. Equipment a user has not accessed gives a "busy" signal;

5. Available memory is less than normal;

6. Programs or data mysteriously disappear;

7. There is suddenly less space remaining on a disk;

8. There is a change in the size of an executable program;

9. A hidden file appears from out of nowhere.

In addition to the "diagnostic" process just outlined, treatment after a system has been infected includes a process called restoration. Restorations differ with the type of virus and degree of infection. The simplest restoration is done by turning off the system power and booting an uninfected original disk, then erasing the virus from the hard disk. One naturally wants to "disinfect" all infected floppy disks at the same time. When data or programs have been lost or corrupted, then this data and these programs must be recovered. Restoration of infected computers connected to a network is quite a bit more complex, and if the viruses in every computer connected to the network are not eliminated at the same time, it is quite possible that all [computers] will immediately become reinfected. This situation requires the expenditure of a great deal of manpower and material resources.

Software To Prevent and Cure Computer Viruses

The precautions and diagnostics for computer viruses just described are all manual, but software specifically for the prevention and cure of computer viruses has now appeared. There are two major categories of this kind of software: one is used for the prevention of computer viruses, and the other is for detecting computer viruses.

For the most part, software used for prevention of infection is RAM-resident, and it monitors all system activity and is on the look-out for the characteristics of various viruses. It can inhibit any scheme that modifies system boot sectors, operating system modules, or application programs. As long as there is some indication of the invasion of the virus, it can immediately issue an alert. There are currently two weaknesses in this sort of program: one, it cannot prevent all viruses, and two, it can issue a false alarm, and just as in the fable about "crying wolf," the consequence of a few false alarms is that the user is no longer vigilant. Even so, as long as this kind of software is used rationally, it can be a powerful tool for preventing invasion by many different viruses.

The other kind of software checks for infection after system contamination. This kind of software usually uses one of two techniques: one is called the "inoculation" or "smallpox vaccination" method, which modifies the system with a self-testing mechanism; when each program is loaded the self-test mechanism checks to see whether the program has been contaminated. The other kind is called the "diary" or "flight recorder" method; this method reads and records key information regarding system sectors that are used, after which, whenever the system is powered on or booted, it compares these "diaries" to catch viruses. Each of these methods has its strong and weak points, but both are effective weapons for detecting viruses.

Computer viruses will get more and more numerous, and the means and tools with which to prevent and cure them will also get more numerous, and also more effective.

The Most Common Computer Viruses

40080222b Beijing JISUANJI SHIJIE [CHINA COMPUTERWORLD] in Chinese No 28, 19 Jul 89 p 34

[Unattributed table entitled: "Most Commonly Seen Computer Viruses"]

[Text]

Virus name: Scores

Origin: USA, Dallas, Electronic Data Systems Co.; Fall 1987

Computer architecture: Macintosh

Type of infection: Infection of general applications programs

Description:
—infects all applications programs;
—increases size of applications programs by 7K bytes;
—creates Note Pad and Scrapbook files in System Folder;
—creates hidden Desktop and Scores files;
—looks to destroy specific file names

Means of transmission:
—exchange of infected disks;
—floppies inserted in infected system

Symptoms:
—system slows down;
—problems in printing;
—system crashes;
—files change size;
—Note Pad and Scrapbook icons change appearance

Potential danger: Data is lost because of system crash

Preventative measures:
—don't exchange disks with other people;
—don't put disks with programs into another person's machine;
—don't run a program with an unknown origin

Restoration:
—back-up all data files;
—erase completely all disks affected by the infection;
—restore System Folder and applications programs from master disks;
—restore data files

Notes: This virus changes the Macintosh icons for the Note Pad and Scrapbook into one with long ears.

Virus name: Lehigh

Origin: USA, Bethlehem, Pennsylvania, Lehigh University; Fall 1987

Computer architecture: IBM PC and compatibles

Type of infection: System infection

Description:
—infects the COMMAND.COM file;
—changes size by about 20 bytes;
—changes date and time of file creation;
—begins activity after 4 replications;
—trashes all system data

Means of transmission:
—sharing of infected floppies;
—clean disk inserted into an infected system

Symptoms:
—size of COMMAND.COM changes;
—all system data is lost

Potential danger: Loss of all data on a hard disk

Preventative measures:
—don't transfer applications programs to system disk;
—don't insert system disk into another machine;
—watch for changes in the date and size of COMMAND.COM

Restoration:
—turn off system power, restore power;
—reboot from original write-protected master disk;
—erase all COMMAND.COM files on the infected hard disk and floppies;
—restore COMMAND.COM from an original master disk

Notes: Because the period of activity is so short (4 infections), there is little opportunity to detect before data is lost.

Virus name: Alameda

Origin: Alameda College, in Oakland, California, USA; Spring 1988

Computer architecture: IBM PC and compatibles

Type of infection: Boot infection

Description:
—installs itself in place of original boot sector;
—stores original boot sector in the first free sector;
—infects through software warmboots;
—there is no indication that the boot sector is not used

Means of transmission:
—inserting clean disk in infected system;
—using a boot disk of unknown origin

Symptoms:
—the boot process slows down;
—system crashes;
—data is lost

Potential danger: Lost data

Preventative measures:
—boot only from a write-protected floppy;
—don't boot the hard disk system from a floppy;
—don't insert boot floppy in another system

Restoration:
—turn off system power, restore power;
—use only a write-protected original boot disk;
—restore the floppy boot sector with the DOS SYS command

Notes: After infection, it does not reprotect the original boot sector, and after the original instructions are inadvertently erased, there could be a boot failure.

Virus name: Pakistani Brain

Origin: Lahore, Pakistan; January 1986

Computer architecture: IBM PC and compatibles

Type of infection: Boot sector infection

Description:
—puts itself in the place of the original boot sector;
—moves the original boot sector to another location;
—adds 7 sectors to store the extra part of the virus;
—to protect itself, it marks modified sectors as unusable;
—it copies itself to all bootable floppies inserted in the computer

Means of transmission:
—use of shared or boot disks of unknown origin;
—accessing (through a directory listing or running a program) an infected disk

Symptoms:
—the volume label of an infected disk appears as "Copyright @ BRAIN";
—the warmboot process slows down;
—abnormal floppy disk access;
—certain versions of DOS crash the machine;
—changes in interrupt vectors

Potential danger:
—crash and loss of data;
—will quickly infect all bootable disks

Preventative measures:
—don't boot floppy disk of unknown origin;
—if you have a hard disk, boot only from that;
—write-protect all bootable floppies

Restoration:
—turn off system power, restore power;
—boot from a clean write-protected bootable floppy;
—list all disk directories, looking for a "@ BRAIN" volume label;
—when you find it, destroy the disk, or;
—run the DOS 'SYS' command to rewrite the boot sector;
—use any relevant application program to generate a new volume label (after this procedure, you will still have 7 bad sectors and the dead virus)

Notes: It is kept alive through software warmboots.

Virus name: nVIR

Origin: Hamburg, West Germany; Summer 1987

Computer architecture: Macintosh

Type of infection: Infects general application programs

Description:
—has appeared in many different forms, each occurrence having different activity characteristics, but the infection technique is extremely simple;
—it places an nVIR resource in the System File; code resource is placed in an application program;
—as soon as the system is infected, each application program that is run will be infected

Means of transmission:
—sharing floppies;
—executing infected programs

Symptoms:
—there are many changes because of the large number of manifestations; in general, symptoms are:
—crashing;
—when launching an application program, a buzz is emitted;
—files are lost

Potential danger:
—data and programs are lost;
—many system crashes

Preventative measures:
—don't share floppies with others;
—keep away from infected systems;
—don't use an original master disk as a working disk

Restoration:
—back-up data files;
—erase infected disks;
—restore programs from the original write-protected master disks;
—restore the data files

Notes: A powerful virus, it can infect all programs in a system within minutes.

Virus name: Israeli

Origin: Jerusalem, Hebrew University; December 1987

Computer architecture: IBM PC and compatibles

Type of infection: Infects general application programs

Description:
—infects all .COM and .EXE programs;
—increases size of programs by 1.8K bytes;
—programs that are infected become resident;
—programs that are run on infected systems will all be infected;
—both floppies and hard disk are infected

Means of transmission:
—infected programs transferred to floppies;
—floppies inserted into infected systems

Symptoms:
—system slows;
—programs will be trashed on Friday the 13th;
—.EXE files will continue to increase in size until they are too large to run;
—available RAM decreases in size

Potential danger:
—certain versions trash all data on a hard disk;
—programs are lost

Preventative measures:
—don't run programs of unknown origin;
—don't exchange floppies that have executable code;
—monitor sizes of RAM allocation and program files

Restoration:
—turn system power off and on;
—boot with an original write-protected floppy;

—erase all executable programs on hard disks and infected floppies;
—restore programs from original floppies

Notes: An error in the original virus caused .EXE files to be infected over and over again until the .EXE files could no longer be loaded into RAM. This problem was eliminated from later versions by an unknown person.

Overview of Computer Viruses

40080222c Beijing JISUANJI SHIJIE [CHINA COMPUTERWORLD] in Chinese No 28, 19 Jul 89 pp 35, 33

[Article by Chen Yousong [7115 1635 2646], Beijing Science & Engineering University: "An Overview of the Computer Virus Situation"]

[Text]

Features and Types of Computer Viruses

The term "computer virus" has recently been appearing regularly in the news media and in the computer profession, and it has attracted wide attention. A virus has always been a microorganism that causes humans or plants and animals to become ill, so how did it come to be associated with computers?

It turns out that some computer software or programs can repeatedly replicate themselves and spread, and they can create various bad consequences that can threaten normal operation of the computer system, just as when viruses replicate themselves within an organism and cause illness. By analogy, people have called this phenomenon a "computer virus."

As far as the varieties of computer viruses are concerned, in a narrow sense, only that which can self-replicate and spread, endangering computer operations, can be called a "computer virus." This narrow definition has been largely adopted in the United States. In a broader sense, aside from the "true virus" just mentioned, there are three other phenomena that can threaten computer operations and that are also called "computer viruses." These are: 1) logic bombs; 2) the trap door; and 3) the Trojan horse. This broader definition is used in Japan.

The logic bomb is intentionally placed there by the author of the program, and it is a time bomb that after a certain amount of time will have the disastrous effect of damaging data; and there is also the kind that does not work according to time, but rather takes the input from a certain kind of activity as the trigger that sets off the bomb.

The trap door is also intentionally manipulated by the software developer. When development of a program is complete and the program is actually running in a computer, the program will accomplish a particular thing only if you know the secret that is used to control operations. Any other person will invariably fall into the program's dead loop or other branch.

The Trojan horse is based on an event from the ancient Trojan War, where troops were hidden in a wooden horse that was pulled into an enemy city; the troops then captured the city by surprise. This term is used to indicate programs that intentionally trick people into making mistakes. The engineer will develop what appears to be a fascinating and reliable program, but when the user runs it at a certain time or after a particular number of times, then a great malfunction from various problems will occur. From the point of view of function, this has similarities with the logic bomb.

The programs just described in a certain sense are all "classic" ways of computer mischief, and when they enter a computer they can destroy data and programs.

The Origins and Prevalence of Computer Viruses

The United States is the source of computer viruses. As long as 20 years ago in science fiction such things as computer viruses were mentioned. The true computer virus is generally recognized to have first occurred 10 years ago at Bell Laboratories in the American Telephone and Telegraph Company. But some people also think that at approximately the same time, during experimental research, scientists at the Palo Alto Research Center of the Xerox Corporation created computer viruses. Whatever, many viruses were created because of the senses of humor of the first group of software developers, who were practical jokers. With the rapid expansion of personal computer networks over the past couple years, the computer virus is becoming a problem in society.

In the United States, this origin of viruses, the scales of the virus presence and the degrees to which computers are being damaged are problems with which everyone is concerned. Because there are currently no data that fully tabulate infections and the damage situation, there is no way to do a complete evaluation of this problem. To take as an example the Apple computers that are equally common in the United States as IBM PCs, among the more than 1 million Apple computers being used in the United States, 25,000-30,000 have been infected. About 5,000 of these cannot be cleansed of the infecting virus. We can see from this the rampant scale of the spreading of viruses.

As of now, the most well-known instances of virus are three: nVIR, Peace, and Scores. Of these, Scores is the most complex. We will use it as an example of how a computer virus actually functions.

After the Scores program has entered a computer system, as soon as it has an appropriate opportunity or after a certain amount of time, it will copy itself and propagate constantly. In this way, the RAM and disk space of the computer will be taken over, ever decreasing the remaining usable space. At first glance, this might seem of little consequence. But as the amount of data needing to be processed grows, requests to use larger amounts of RAM will lead to problems. Because it was first occupied

by the virus, the RAM that could have been used issues a fault that causes the program to run wild, leading to the destruction of data. Because this kind of fault cannot be accounted for previously, problems become more complex when they occur, and one invariably falls into the predicament that elicits "I don't know what to do" and "what is happening is really weird." What is more, it is no easy matter to discover this virus. Therefore, the reliability of such computers is lessened, as its operation normally becomes ludicrous and unfathomable by anyone.

Japan has similarly been invaded by computer viruses. One that has recently made quite a stir is the virus that infected the Nippon Denki PC-VAN [value added network] network, which was discovered in the middle of August 1988. What follows is an outline of the event.

PC-VAN is the largest personal computer network in Japan. In the middle of August 1988 all members of PC-VAN were able to see on their screens a document of uncertain meaning. Authorities who became suspicious of this traced this strange phenomenon, and found that it was a secret signal used by a "criminal" to steal the passwords of other members (they are encoded text). There were 13 members whose passwords had been stolen. But this affair certainly did not have disastrous consequences, as this was simply a matter of the "criminal" fooling around.

Through the means of computer communications via E-mail, the culprit sent programs containing an "agent" to many non-specific people. Network people who were interested in this program only had to turn on their own personal computer and this "agent" would immediately sneak into the operating system of the personal computer. Then, when this person had connected to PC-VAN, the "agent" would suddenly go to work, displaying a nonsense document. To render this clearly, the user would enter his encoded password, and the "criminal" could then steal it. That was his plan.

Newspapers in Japan widely reported this affair using such sensational headlines as "Computer Viruses Have Now Entered Japan" and "A Virus Program That Threatens Personal Computers." But according to the previous definition, the phenomenon in the PC-VAN affair was not a true computer virus, but rather was a kind of Trojan horse. This was a new way to show off with a practical joke using this personal computer communications network as a new medium.

It should be pointed out that practical jokers are crazy about personal computers. They are very knowledgeable, and are just waiting for the opportunity to illegally get into computer networks. The Trojan horse set by the practical joker is closely related to true computer viruses. Some of the problem programs they have written invariably become true computer viruses.

The Prevention and Cure of Computer Viruses

As of now, whether in the United States or in Japan, there are yet no cases where computer viruses have been used to do serious criminal computer activity. This is because the majority of viruses are created by conceited practical jokers who want to show off their brilliance. There is therefore a great deal of humor involved.

But as the information society grows, the spread of computer networks will abound in private areas, and it will be difficult to guarantee that the future will not see computer viruses used to invade networks for serious criminal activity. Particularly for some military networks or those in critical sectors, as soon as a virus has invaded, the results could be unimaginable. This is why ways have to be conceived to prevent and cure computer viruses.

As computer viruses are wielding their despotic power, there are also appearing some effective prescriptions for curing the viruses—"vaccine" programs. There are six "vaccine" programs in the United States just to prevent and cure viruses on the Apple microcomputers. There are also programs under development to discover viruses. And a true "vaccine" program is about to appear that combines the function of detection, cure, and restoration, and can be used to recover from viruses.

These "vaccine" programs are for the most part all effective against those viruses already discovered: nVIR, Peace, and Scores. They will have to be altered in use for the new viruses. If we were to say that it takes 1,000 hours to create a computer virus, then in an hour's time it will be possible to accomplish the work of curing viruses by discovering the virus and running a vaccine program to cure the symptoms.

With the spread of "vaccine" programs in the United States, and a deeper understanding of computer viruses, computer viruses can now be treated in a detached manner. In Japan, where computer viruses have been rare, the PC-VAN incident was overblown and led to panic.

To end, I will describe a measure to prevent viruses. One means of doing so, when using public domain software, is to not irresponsibly use electronic mail to send or use programs of unknown origin. So that on the off chance you do become infected with a virus, to keep from doing damage, you should do regular back-ups of important programs and data: that is, store them after copying. As soon as a virus invades, because there will be changes in the size of the programs (normally, a computer virus is 2-7K bytes), the virus can be detected by the change in program size. People are now trying to think of ways to uncover viruses even sooner.

To summarize, with the growing presence of computer networks, the consequences of computer viruses will become more serious, and this cannot be treated lightly. But the means of prevention, detection, and cure of

viruses are also constantly improving. For this reason, computer viruses need not be feared.

Virus Attacks on Computers

40080222d Beijing JISUANJI SHIJIE [CHINA COMPUTERWORLD] in Chinese No 28, 19 Jul 89 pp 37, 40

[Article by Li Juyi [2621 1565 6230]: "The Virus Attack on Computers"]

[Text] When the computer network Internet, spanning the entire United States, was infected on 3 November 1988, approximately 6,000 minicomputers and workstations based on Unix were infected. The attack by the computer virus led to a loss of computer time, as well as the expense of restoring the infected machines, all of which resulted in losses to computer users of about US$92 million. A cause for joy, however, was that on the occasion of this large infection the computers of DEC [Digital Equipment Corp.] were relatively unharmed. On Internet, the virus used a weakness in the Berkeley 4.3 Unix E-mail system to invade the network, but that weakness did not exist in the Digital version of Berkeley Unix called Ultrix. This weakness in E-mail makes the computer act as a program that is running electronic information that exceeds a particular byte count. If the virus exceeds a particular byte count, it then quickly copies itself, thus damaging the object of the attack through a virus program.

Because the carrier of the virus is the computer network, within a few minutes the virus was able to infect computers in academic research centers, and could even reach computers at Cambridge, MIT, and at the Lawrence Livermore [National] Laboratory in California. The Internet virus was certainly not the first computer virus to spread through a computer network, but it might have been the first virus to attack a network interconnecting computers in the American national defense sector. Many people were shocked by this fact—minicomputers have become victims of the attacks of computer viruses.

It Is Even Hard for Minicomputers and Workstations To Avoid Viral Attacks

Computer security experts feel that if viral attacks were to lead to the collapse of Internet, then it would be a fact that even minicomputers and workstations can hardly avoid viral attacks and infection by similar programs. These virus programs are generally quite small, and it is even possible that in the beginning these programs were designed to be beneficial (there are materials that suggest that the Internet network virus was designed to repair the E-mail weakness), but normally viruses lead to paralysis of the system and loss of data. As far as the virus is concerned, the damage to the computer is caused by the virus' self-replication. Typically, as soon as a computer begins operation, the virus can quickly infect the operating system from an infected disk. A Trojan horse is usually a useful program, but this program will contain a hidden threat to the computer system, a threat that can even be serious. The logic bomb is also a program, and it is deadly in its damage to computer data resources, as it carries inside itself a time bomb, which after loading of the program "ignites" the bomb long afterward.

Because there is no computer system that can avoid a viral attack, it is important that systems check thoroughly for virus clues (the restoration of a single system in a network from a viral manifestation that appears in a particular system can seldom fundamentally solve this problem). Minicomputers (and especially such minicomputers running proprietary operating systems as Digital's VMS) have better security than PC computers running under MS-DOS. To prohibit and restrict computer activities instigated by computer viruses, in fact, any minicomputer operating system has distinct advantages over the basic PC operating system. On PCs, a virus can rewrite the file allocation tables (FAT) of a file on a PC, by which it can erase an entire PC hard disk. On a VAX or other minicomputer, which have segmented instruction sets, the user and the computer virus can only write or erase data in its own memory space on the system disks, so it would be extremely difficult for a virus to rewrite an entire disk.

Regarding this point, some people have asked: If all this is true, why were so many minicomputers attacked by the Internet virus? Actually, the adversary with which the Internet network has most trouble dealing is a worm. A worm is a short program that can successively and rapidly copy itself, while a virus copies itself into the operating system.

Viral Damage to Data

There are different types of computer viruses. One is a virus that primarily attacks PCs, most often manifest in damaged data; another is a worm, which attacks minicomputers. A worm normally damages a system, and in comparison with a virus, it can take less time to restore a worm-damaged system.

Sherizen and other computer security experts believe that the fact of the Internet network attack shows that Unix security is rather weak. Digital said that 10 percent of its users are using Ultrix, and another 10 percent are using Unix from other vendors. But because Digital is promoting its DECstations, based on RISC architecture and running Ultrix, the number of Ultrix users will probably increase from now on. However, the Internet virus did not attack systems running other major versions of Unix and the AT&T System V, and system managers and computer thieves who are designing computer viruses all know of weak points in those two versions. A definite problem with Unix (that has still not been fixed) is the user category called "superuser," under which classification the user can read and write at any place in the system. When it is necessary to simply read and write what a user needs, the program can enter the superuser state. In this state, one can do system calls by SETU ID (set user ID) and SETG ID (set group ID). Any

program can thus be given unlimited privileges, which is extremely dangerous, especially with such programs as the Trojan horse that can damage the system.

A computer weakness requires that system managers prove the reliability of their programs, but because Unix provides an open environment in which programs can be quite portable, it is difficult to achieve that. The debate about Unix security goes like this: Some people feel that "Unix security" is an oxymoron, while others are extremely sensitive to the Unix security question. Actually, the weakness of security in Unix is in the fact that a user can look at the source code of Unix and can test the Unix security measures. Every operating system has a superuser account or a system manager account, which are provided for free access to the operating system. There are quite a few limitations in the form taken by the Ultrix superuser account, and in addition to the superuser account there are also different levels of privilege. As far as network users are concerned, the latest version of Ultrix does strict checking of remote commands issued from other computers.

The most recent versions of Unix have made great advances in light of user concern about problems with operating system security. For example, secure versions of Unix (as for example AT&T's System V/MLS) provide many levels of security. AT&T advertises that the enhanced version of System V, System V/MLS, provides many levels of security.

"Vaccines" now exist to cope with these computer viruses that are so frightening people. They are currently only available for PC and Macintosh computers, which both support RAM-resident programs, something minicomputers do not. One would imagine that vaccines for minicomputers could also be developed, but they would be triggered into operation by a user or by the system manager, and would not be a self-generated minicomputer "bodyguard." To implement this kind of "bodyguard" function on a minicomputer, a minicomputer virus vaccine must use the paging process; this is a process in which each portion of a program is force-written into the required memory. This would greatly reduce the operational speed of the computer.

Vaccines Are Certainly Not All-Purpose

To the PC and VAX users, what is more important is that vaccines are themselves a subject currently under debate. The vaccines that we use today are all based on the viruses that were discovered in the past, and these vaccines cannot protect computer users from attack by newly generated viruses. The basic problem lies in the fact that there is no "universal vaccine" that can be used on any computer and that can guard against viruses on all machines.

Because there is no rapid solution to this problem with viruses, Digital users have no choice but to use tested or proven methods to protect the user's own VAX. The majority of security needed for VAX users is already implemented in the VMS or Ultrix systems, and users should understand how to use this security. All major operating systems with security measures have levels suitable for users and system managers to do system read/writes, and it is possible to trace who has used or who has tried to use an audit trace function on a particular file.

Aside from the special security measures provided by the operating system, security experts have come up with several management strategies that system managers can use:

1. Use the write-protect function provided by VAX drives;

2. During the software development process, use a transaction journal, by which is meant that at the same time as software developers at a company change program code, they can prohibit use of trapdoors, that is, man-made traps through which one might enter the larger application program or operating system;

3. There should be a strict investigation made in front of hired personnel or system managers, and when they have left the company, they should be immediately prohibited from reading and writing in the system.

In general, system management personnel should carefully consider the security situation of their own system, and software retailers must strictly test products; although the majority of Berkeley 4.3 Unix retailers have solved the weakness of the E-mail, virus infections have by no means been stamped out. As for software that has yet to appear, the focus of the Digital testing procedure will be on security. The company has set up an organization to develop security standards, and Digital has taken great interest in the government C2 standard for Ultrix. That C2 standard is a national-defense security standard requiring monitoring of user activity.

Another aspect to the ability to obtain hardware and software provider help is that when a system is newly infected by a virus, one can do a quick restoration, which additionally is training for the user. Many companies are working hard in this area, and Digital in particular is very cognizant of this, as they have recently published a free guide to Ultrix security problems. In one part of the Digital user training process having to do with viruses and other programs that attack systems, the company has exposed some rumors, such as one in which many users are worried that PC viruses will enter VAX computers, which is impossible. Because of essential differences between the operating systems of the PC and the VAX, even when a VAX is the server on a PC LAN [local area network], it cannot transfer a virus to other PCs.

Naturally, what most worries Digital users is what is going to happen next, as they see to what extent the Internet virus was able to spread, knowing that the computer criminals will further perfect or modify their viruses. No matter what, it would be mistaken to believe that a good edition of the operating system will avoid

virus attacks. People are predicting that operating systems over the next few years will more rigorously determine user privileges, and that there will be less interest by users in having particular access throughout the network.

Conclusion

The computer virus has become an effective trick for computer criminals, and it is also the most serious method by which to attack computers. At present, the effective prohibition of viral infections, and even the eradication of viruses, is a problem of concern to every computer activist and even to governments.

Method Described for Detecting a Shell Virus

40080222e Beijing JISUANJI SHIJIE [CHINA COMPUTERWORLD] in Chinese No 28, 19 Jul 89 p 38

[Article by Xi Hongyu [1153 4767 1342] of Beijing University, Department of Mechanics: "Methods of Detecting Shell 'Viruses'"]

[Text] With the ever broadening application of computers, computer crime is also on the increase. One type of computer crime—the computer virus, is no longer a distant event. In particular there was the computer virus attack scheme that occurred in the United States in the latter half of 1988, which has created quite a stir in the computer world. We have even discovered some computer "virus" infections in China [see JPRS-CST-89-014, 18 Jul 89, pp 46-47].

PC Viruses

There is a malignant virus spreading among PC and compatibles at some institutions and research centers in Beijing. It can infect .COM files that run under the DOS operating system (such as MS-DOS, PC-DOS, and CC-DOS). Computer software personnel at Beijing University have traced and isolated this virus (which is being provisionally known as "Type-B"). Some software tools have been [domestically] developed especially to detect this kind of virus [see JPRS-CST-89-018, 22 Sep 89, pp 75-76]. At the same time, by analyzing and dissecting this virus, the transmission and destructive principles behind this virus have been discovered, and tools are being provided to restore software that has been infected by the virus.

Testing for Viruses

Looked at broadly, there are four types of "computer viruses": those in operating systems, those in shells, the invasive type, and those in source code. The Type-B that has been discovered is a shell type. Each time an infected program is used, it will look on the disk for an uninfected program to infect, then copy the infected portion into the program. This causes the program to execute the virus when first running the program, which accomplishes the goal of constant propagation. All computers that have been infected by this virus become a new source of infection, and since all floppies used on the system become infected, there is repeated dissemination. From the point of view of viral dissemination, infection is not necessarily through copying (naturally, copying software is the most commonly seen way of infection).

In light of the modes just discussed, we will describe an easy way to detect whether or not your hard disk has become infected with the Type-B virus (similarly with floppies).

1. Format a floppy that has no bad sectors, and copy onto it several regular COM files.

2. Record the lengths of the files.

3. At the DOS A> prompt, run a series of .COM files that are on the hard disk (you don't have to run them all the way; just load them and exit to the operating system).

4. In a normal fashion, use the DIR A: command to check the lengths of the .COM files on the floppy.

5. After you have run all the .COM files on the hard disk, and the lengths of the .COM files on the floppy never change, we can generally affirm that the hard disk has not been infected.

6. If the .COM files on the floppy increase in size, then we can probably say that the hard disk has become infected with some kind of virus, and if the added length is 648 bytes, we may say that the virus is Type-B.

7. All steps just described involve running .COM files from the C: hard disk while at the A> prompt.

If you suspect a different virus, you can still use this method, but add some .EXE files and some data files to the floppy, and some source code, but nothing more. Otherwise, it will not be easy to see changes in the lengths. It is now necessary to run .EXE programs that are on the hard disk.

Before you finish, use the CHKDSK command to see if the floppy has any bad sectors. If it does, you must proceed carefully, as some viruses are placed in areas falsely marked as bad sectors.

Type-B will also completely destroy some .COM files (about 10 percent), and when you next run this damaged software it will seem as if you have just turned on the computer. That is, it first checks available RAM and peripherals, then loads the BIOS and DOS from disk. Thus, the original functions of this software are lost, nor is there any way to recover them. To confirm this, you can tell easily using the following method.

(Using DISKCOPY.COM as an example:)

```
C>DEBUG DISKCOPY.COM
-U
XXXX: 0100 JMP F000: FFF0
...
-Q
```

If the first statement is JMP F000, that is, a jump to the physical address FFF0, which is the location of the first instruction to be run at power-up for the Intel 80-series of microprocessors, then the apparent "cold boot" phenomenon can occur.

A great deal of damage can arise from this situation, and if the back-up files are also damaged, this could lead to even greater damage. This kind of virus is therefore called a "harmful virus," while the average "benign virus" will only spread itself and take up space in RAM and in external storage. In that case there will appear some nasty or irrelevant information on the screen, some even affecting normal display, and still others will affect the efficiency of execution, seriously causing normal operations to nearly cease.

We have also noticed that programs infected with and damaged by the Type-B virus will show no change in the time of file creation. Because at the time of infection it has stored away the time of file creation, it then restores this after infection, so it is not easy to tell that the infection has occurred. Files that have been damaged do not change in length, an important point to be aware of.

The detection method outlined above is a general method that can be used when it cannot be determined whether infection has occurred or what the mode of infection has been. When the principles of the virus have been understood, you can create a series of software tools that hunt down and eliminate viruses.

The VTEST.EXE we have come up with is an automatic search and analysis tool, where when the user selects the disk to be checked (floppy or hard disk), the software will automatically search files from the root directory through the subdirectories, looking for evidence of the Type-B infection or damage, after which it reports on its results. The automatic restoration tools can not only detect files that have been infected and damaged, but can also disinfect infected files, eliminating the virus portion and restoring their original normal operation. In this way, it does not matter whether the user is a trained or beginning software person, everyone can quite confidently use this tool, and he will not be leaving a single file with the Type-B virus. This tool can also check newly purchased and other software that has been used on a computer to guard against the intrusion of a virus from outside, which is the goal of prevention.

Preventative Measures

Computer viruses are not mysterious, after all. Simply by discovering the virus and analyzing its means of entry, you can certainly find the means with which to combat it. The only problem is that before effective means were discovered and developed, the viruses caused many users a great deal of trouble and loss. We should therefore face up to this problem, because it is not a simple problem of pure computer science, but is now a serious problem for society.

Computer viruses differ from the biological kind in that nearly all computer viruses are intentionally created by man, some being out of control upon dissemination, even by their creator. The concept should be considered as a new kind of crime, but because China has no "software laws," it is hard to manage many problems in this area. Even if we had such laws, there would always be some computer "mad men" who would jump at testing the law or finding loopholes in the law. We therefore call upon all persons working with computers to strengthen their own moral fortitude, and to improve their professional moral concepts. Then there could be no intentional introduction, creation, nor dissemination of any kind of virus.

To reduce the possibility of infection, we recommend the following:

1. Each vendor of software must be responsible for the products he sells, guaranteeing that none contain viruses (we recommend that "software laws" hold sellers or marketers of software intentionally or unintentionally having viruses responsible for the consequences).

2. Do not arbitrarily copy software, and software that you must use should certainly be purchased from a known seller.

3. Computers in important departments should be isolated from the outside world, and, to the greatest extent possible, should not be loaded with new software. Also, do not casually use disks used on other machines on the machines in question (and that includes game software).

4. Use virus detection software and tools of various types to periodically test files on computer hard disks; to whatever extent possible, load new software on a hard disk only after it has been checked.

5. Immediately isolate a virus upon discovery, disinfect it quickly, and look for its source.

6. Pertinent sectors of the state should set up "computer hospitals" at a national level that periodically distribute "vaccine" reports and alert users at large. At the same time, they could monitor the development of viruses both in China and abroad, researching the theories of dealing with all types of viruses and actual problems. They could produce anti-viral software tools. For particularly difficult "symptoms," they could arrange for "group diagnoses." The urgency and possible consequences for dealing with the virus problem in this way are as important as those at a hospital for saving lives.

New Virus and Anti-Viral Measures Described

40080222f Beijing JISUANJI SHIJIE [CHINA COMPUTERWORLD] in Chinese No 28, 19 Jul 89 p 39

[Editorial comment]

[Text] The "round point" virus is one computer virus that has been discovered in China. It is primarily transmitted among IBM PC/XTs and ATs, and its symptom is

a small sphere bouncing back and forth like a ping-pong ball on the screen in text mode on infected computers. It is similar in the Chinese mode, but more serious as the entire screen becomes a coarse light dot like a "ping-pong" ball going back and forth, rolling all the time, which completely negates the intended screen contents.

Because the existence of this virus program (and its continual replication) takes over so much CPU time for its execution, the computer appears to be "busy," which significantly lowers performance to an intolerable level. Although this virus does not damage the execution of applications programs (they can run to their completion), the virus continues to run and can only be temporarily stopped by rebooting the computer. This virus is quite contagious, as it is transmitted even with the DIR command to check a floppy's contents, as well as by copying a floppy. This virus accomplishes its destructive activity by modifying the called locations of MS-DOS or PC-DOS disk interrupt 13 and the clock interrupt 8.

In view of this situation, we have written some articles pertaining to the diagnosis of, elimination of, and vaccination against this round-point virus. We hope that these measures can resolve the thorny problem for users of computers infected by this virus.

Discovery of Another Chinese Virus, Appropriate Measures

40080222g Beijing JISUANJI SHIJIE [CHINA COMPUTERWORLD] in Chinese No 28, 19 Jul 89 pp 39-40

[Article by Yu Dong [0151 2639], China University of Science & Technology, Radio Department: "Analysis of a Computer Virus and Methods for Its Elimination"]

[Text] Many microcomputers (PCs) at the China University of Science & Technology (CUST) have become infected by a virus, the particular symptoms of which are: a small dot of light (CRT output code 07) jumps up and down on the screen, and bounces off certain characters all around the screen, after which it keeps on bouncing. It is very like the motion of a ping-pong ball on a table tennis table. It does not generally affect the execution of a program, but the speed of that execution is reduced.

The virus generally enters memory during booting and loading of an infected disk. After a detailed analysis of floppy and hard disks having the virus, we discovered that the disk boot sector had been modified by the virus. The specific command for DEBUG is as follows:

-L cs: 100 a 0 1

where 'a' represents the drive to check.

The infected routine in the boot sector appears as follows:

0F18:0100 EB1C	JMP	011E
0F18:0102 90	NOP	
0F18:0103 49	DEC	CX
0F18:011E 33C0	XOR	AX,AX
0F18:0120 8ED0	MOV	SS,AX
0F18:0122 BC007C	MOV	SP,7C00
0F18:0125 8ED8	MOV	DS,AX
0F18:0127 A11304	MOV	AX,[0413]
0F18:012A 2D0200	SUB	AX,0002
0F18:012D A31304	MOV	[0413],AX
0F18:0130 B106	MOV	CL,06
0F18:0132 D3E0	SHL	AX,CL
0F18:0134 2DC007	SUB	AX,07C0
0F18:0137 8EC0	MOV	ES,AX
0F18:0139 BE007C	MOV	SI,7C00
0F18:013C 8BFE	MOV	DI,SI

whereas the routine in an uninfected disk is:

-u 100		
0F18:0100 EB34	JMP	0136
0F18:0102 90	NOP	
0		
0F18:0136 FA	CLI	
0F18:0137 33C0	XOR	AX,AX
0F18:0139 8ED0	MOV	SS,AX
0F18:013B BC007C	MOV	SP,7C00
0F18:013E 16	PUSH	SS
0F18:013F 07	POP	ES
0F18:0140 BB7800	MOV	BX,0078
0F18:0143 36	SS:	
0F18:0144 C537	LDS	SI,[BX]
0F18:0146 1E	PUSH	DS
0F18:0147 56	PUSH	SI
0F18:0148 16	PUSH	SS
0F18:0149 53	PUSH	BX
0F18:014A BF2B7C	MOV	DI,7C2B
0F18:014D B90B00	MOV	CX,000B
0F18:0150 FC	CLD	
0F18:0151 AC	LODSB	
0F18:0152 26	ES:	
0F18:0153 803D00	CMP	BYTE PTR [DI],00

The originator of this virus has a trick in the disk boot sector. The system does its self-checks and initialization normally upon power-on, whereupon it reads in the boot sector. If the boot sector has been damaged, the system

cannot continue its normal initialization. But the virus causes the system to install itself in the highest part of RAM before looking for IBM BIO.COM and IBM DOS.COM, where it occupies a total 2K RAM. Only then does it begin its true initialization, checking to see whether the disk has the IBM BIO.COM and IBM DOS.COM, from which it proceeds with the normal initialization process.

We know that there is part of COMMAND.COM that is resident in the highest part of memory, but the virus moves that down 2K. Working in this way, there is only a 2K reduction in RAM over that possible for an integral IBM PC. We can see this with the SYSTEM INFO function of PCTOOLS. When DOS checks its memory it presumes the transient portion of COMMAND.COM is at the highest point in RAM, so the RAM value it checks will be 2K less than that discovered upon power-on.

There is another characteristic. We will sometimes discover that RAM is not only 2K less, but because each time the virus in the boot sector does its initialization, it will take another 2K away from RAM. After it has run a few times, the amount of space it occupies naturally increases.

The key to this virus is in its modification of the interrupt vector table, whereby in the system initialization process it alters the INT13 address, which then points to a location 2K bytes below the highest point of RAM. With every disk access, a portion of the virus code is run first, then execution continues with the true INT13.

All users who find themselves with this virus have discovered that the virus does not just run all of a sudden, but rather wakes up under certain conditions. We can see in a disassembly of the code that there are two conditions: 1) contact with INT13; and 2) a certain amount of time passing (part of the code of the modified INT13 is provided as an appendix).

When the two conditions are satisfied, the virus then modifies the INT8 entry. INT8 is a hardware interrupt that is issued 18.2 times per second. It is generated by the 8253-5 CNT 0 on the IBM PC motherboard, then is sent to the IRO input of the 8259A interrupt controller. Therefore, each time-reference signal generates an interrupt request, which is used to calculate time of day.

In the modified INT8, we can see that there is first a portion of code having to do with display, the function of which is to generate a moving point of light. Jump to the true INT8 entry occurs only after this. Because INT8 is generated 18.2 times per second, we see a point of light that is always in motion, which jumps on the screen.

An important characteristic of the virus is its self-replicating function. Transmission of the virus is primarily dependent upon that characteristic. It is also accomplished through INT13, whereby it first determines whether the disk has the virus, and if not, then modifies the disk boot sector, where it installs a portion of the virus routine. It then moves to the first unused sector on the disk, where it enters the damage mark 'FF7', after which it copies itself onto the disk. That is why even when your disk is not a system disk, upon initialization, if the disk has been infected, the virus routines will still be loaded into RAM.

This virus belongs to the category of "benign viruses," as it does not generally affect the results of a program's execution. Because it lengthens the code of the INT8 routine, this adds to the time of execution, which somewhat slows down the execution of user programs.

The elimination of this virus is also fairly easy, the specific method for which is as follows:

Use the EDIT function of PCTOOLS to check sector 0 on a disk, where we will see such designations as 'PCTOOLS' or 'IBM X.X', after which use the PCTOOLS SEARCH function to look for the string you have just seen. When you find the first occurrence, keep going. In later sectors make a note of the sector numbers in which you find this string. Convert that to hexadecimal, exit PCTOOLS, and enter DEBUG. Type in:

-L cs: 100 a b 1

where 'a' represents the designation of the drive you wish to modify, and 'b' represents the hexadecimal sector number you had just found. Then type:

-W cs: 100a01

You are half through. Because the virus will add the sectors in which the virus is resident to the list of bad sectors, this ensures that later data will not erase the data in this sector. If this sector is not modified, this sector will no longer be usable (without reformatting the disk). On the FAT area of the disk, we should therefore change the damaged indicators in this sector from 'FF7' to'000', indicating that these sectors are available for use. Restoration work is now complete. Please note that you should be careful with operations on the boot sector of a disk, and do another write to this sector when there are no errors in data; otherwise there could be trouble in the future.

We can see from the foregoing analysis that the primary point of departure for this program is modification of INT13 and of the disk boot sector. This is the fundamental starting point for most personal computer viruses, and if we understand this, it is not difficult to come up with the means to deal with viruses.

3F80:00D0 1E	PUSH	DS: The modified INT13 entry
3F80:00D1 06	PUSH	ES
3F80:00D2 50	PUSH	AX
3F80:00D3 53	PUSH	BX
3F80:00D4 51	PUSH	CX
3F80:00D5 52	PUSH	DX
3F80:00D6 0E	PUSH	CS

3F80:00D0 1E	PUSH	DS; The modified INT13 entry
3F80:00D7 1F	POP	DS
3F80:00D8 0E	PUSH	CS
3F80:00D9 07	POP	ES
3F80:00DA F606F77D01	TEST	BYTE PTR [7DF7],01
3F80:00DF 7542	JNZ	0123
3F80:00E1 80FC02	CMP	AH,02
3F80:00E4 753D	JNZ	0123
3F80:00E6 3816F87D	CMP	[7DF8],DL
-u		
3F80:00EA 8816F87D	MOV	[7DF8],DL
3F80:00EE 7522	JNZ	0112
3F80:00F0 32E4	XOR	AH,AH
3F80:00F2 CD1A	INT	1A; Read clock
3F80:00F4 F6C67F	TEST	DH,7F
3F80:00F7 750A	JNZ	0103
3F80:00F9 F6C2F0	TEST	DL,F0
3F80:00FC 7505	JNZ	0103
3F80:00FE 52	PUSH	DX
3F80:00FF E8B101	CALL	02B3; Determine whether to modify 2INT8 [??]
3F80:0102 5A	POP	DX
3F80:0103 8BCA	MOV	CX,DX
3F80:0105 2B16B07E	SUB	DX,[7EB0]
3F80:0109 890EB07E	MOV	[7EBO],CX
-u		
3F80:010D 83EA24	SUB	DX,+24
3F80:0110 7211	JB	0123
3F80:0112 800EF77D01	OR	BYTE PTR [7DF7],01
3F80:0117 56	PUSH	SI
3F80:0118 57	PUSH	DI
3F80:0119 E81200	CALL	012E; Copy virus
3F80:011C 5F	POP	DI

3F80:00D0 1E	PUSH	DS; The modified INT13 entry
3F80:011D 5E	POP	SI
3F80:011E 8026F77DFE	AND	BYTE PTR [7DF7],FE
3F80:0123 5A	POP	DX
3F80:0124 59	POP	CX
3F80:0125 5B	POP	BX
3F80:0126 58	POP	AX
3F80:0127 07	POP	ES
3F80:0128 1F	POP	DS
3F80:0129 EA59EC00F0	JMP	F000:EC59; True INT13 entry

One Way To Disinfect a Computer Virus

40080222h Beijing JISUANJI SHIJIE [CHINA COMPUTERWORLD] in Chinese No 28, 19 Jul 89 p 41

[Article by Zhang Yingqi [1728 2019 0796], Huaibei Bureau of Mining, Computing Center: "One Method for 'Disinfecting' Computers With Viruses"]

[Text]

Virus Diagnostics

Depending on the distribution of the virus over a disk, we can know whether infection has occurred just by using DEBUG or PCTOOLS to read the boot record of a disk. The clearest indication is that the last 128 bytes of the correct boot record generally contain boot error messages, while this location on infected disks simply contains random bytes of unclear purpose. This is a clear indication.

We present below the beginning and end of the correct boot sector as read by DEBUG:

The beginning of a virus-bearing boot sector is as follows:

It is best to use DEBUG and PCTOOLS as tools for disinfecting, but DEBUG can be used alone.

```
-L 100 0 0 1

-D 100 13F
1160:0100  EB 2C 90 49 42 4D 20 20-32 2E 30 00 02 02 01 00   .,.IBM  2.0.....
1160:0110  02 70 00 00 02 F0 02 00-09 00 02 00 00 00 00 00   .p..............
1160:0120  0A 0F 02 25 02 09 2A FF-50 F6 0F 02 C0 19 FA 33   ...%..*.P......3
1160:0130  C0 8E D0 BC 00 7C 8E D8-A3 7A 00 C7 06 78 00 21   .....|...z...x.!

-D 280 2FF
1160:0280  0D 0A 4E 6F 6E 2D 53 79-73 74 65 6D 20 64 69 73   ..Non-System dis
1160:0290  6B 20 6F 72 20 64 69 73-6B 20 65 72 72 6F 72 0D   k or disk error.
1160:02A0  0A 52 65 70 6C 61 63 65-20 61 6E 64 20 73 74 72   .Replace and str
1160:02B0  69 6B 65 20 61 6E 79 20-6B 65 79 20 77 68 65 6E   ike any key when
1160:02C0  20 72 65 61 64 79 0D 0A-00 0D 0A 44 69 73 6B 20    ready.....Disk
1160:02D0  42 6F 6F 74 20 66 61 69-6C 75 72 65 0D 0A 00 69   Boot failure...i
1160:02E0  62 6D 62 69 6F 20 20 63-6F 6D 30 69 62 6D 64 6F   bmbio  com0ibmdo
1160:02F0  73 20 20 63 6F 6D 30 00-00 00 00 00 00 00 55 AA   s  com0.......U.
```

```
-L 100 0 0 1

-D 100 13F
1160:0100  EB 1C 90 49 42 4D 20 20-32 2E 30 00 02 02 01 00   ...IBM  2.0.....
1160:0110  02 70 00 00 02 F0 02 00-09 00 02 00 00 00 33 C0   .p............3.
1160:0120  8E D0 BC 00 7C 8E D8 A1-13 04 2D 02 00 A3 13 04   ....|.....-.....
1160:0130  B1 06 D3 E0 2D C0 07 8E-C0 8E D0 7C 8B FE B9 00   ....-.......|....

-D 280 2FF
1160:0280  A3 F5 7D 8B 36 F9 81 E9-08 01 C3 81 3E 0B 80 00   ..}.6.......>...
1160:0290  02 75 F7 80 3E 0D 80 02-72 F0 8B 0E 0E 80 A0 10   .u..>...r.......
1160:02A0  80 98 F7 26 16 80 03 C8-8B 20 00 F7 26 11 80 05   ...&..... ..&...
1160:02B0  FF 01 8B D0 02 F7 F3 03-C8 89 0E F5 7D A1 13 7C   ............}..|
1160:02C0  2B 06 F5 7D 8A 1E 0D 7C-33 D2 32 FF F7 F3 40 88   +..}...|3.2...@.
1160:02D0  F8 80 26 F7 7D FB 3D F0-0F 76 05 80 0E F7 7D 04   ..&.}.=..v....}.
1160:02E0  8E 01 00 8B 1E 0E 7C 48-89 1E F3 7D C6 06 B2 7E   ......|K...}...~
1160:02F0  FE E8 0D 02 00 0C 00 01-00 8E 02 00 57 13 55 AA   ............W.U.
```

1. To determine the position of the first sector among the disk data sectors occupied by a virus: there is a section of special code starting with the 223rd byte in this sector of the virus—"1E 50 53 51 52 0E 1F B4 0F." You can use the 'F' command of the PCTOOLS disk functions to accurately search for this byte string, or look for it with the 'S' command of DEBUG after loading a full or partial disk. In this way you can arrive at or convert to the relevant sector number 'S' (for the sake of convenience, for the remainder of this text we presume a 360K-byte floppy, and the virus sector S equals 12, or 0CH). You can use a formula to derive the cluster in which this sector resides (C = 2), and the FAT for the relative position of this sector has written 'FF7' for the damaged sectors. The conversion formula is:

360K-byte disk:	S = 2C + 8;
10 megabyte hard disk:	S = 8C + 33;
20 megabyte hard disk:	S = 16C + 49.

2. Modify the damaged sector indicator FF7 in the FAT. Because the length of FAT cluster elements in DOS 2.1 is 12 bits (it is written as three hexadecimal digits), and because it has its own special rules for storage in the FAT, it can be hard to read. The method for determining the position of the 'FF7' is as follows:

Use DEBUG to load the FAT table into memory:

-L 100 0 1 2

Multiply the cluster number (2 in this example) by 1.5 and round off (3 here), then convert that to a hexadecimal number and use that number in the FAT to find the positioning bytes (when the FAT is loaded, it begins at an offset of 100H from the address of the current number, so 100H must be added, yielding 103H for this example). Select the character from this byte position, keeping in mind that on this computer a hexadecimal value has its high value behind and its low value in front, so you must adjust the sequence. If the resulting value in the original boot sector (note that this is not "cluster number") is an even number, then use the lower three digits and if an odd number, the higher three digits; then use the 'E' command to change the 'FF7' to the empty cluster designator'000'. For example,

-L 100 0 1 2

-D 100 10F

1160: 0100 FD FF FF F7 0F 00 00 00—00 00 00 00 00 00 00 00...

-E 103 00 00

-D 100 10F

1160: 0100 FD FF FF 00 00 00 00 00—00 00 00 00 00 00 00 00...

-W 100 0 1 2

It should also be noted that when you finally use the 'W' write command, its parameters should be completely the same as those of the 'L' command.

3. Rewrite the correct boot record in the second sector of the virus location (here, 0DH) to sector 0:

-L 100 0 0 1

-W 100 0 0 1

4. Find two other sectors that do not contain the virus (here, using 0EH and 0FH) to write over the two virus sectors (0CH and 0DH in this example.

-L 100 0 E 2

-W 100 0 C 2

The "disinfection" process is now complete. We have processed several hard disks and dozens of floppies in this manner, after which the virus was silenced without a trace.

Program Listing for Detoxifying, Vaccinating Disks

40080222i Beijing JISUANJI SHIJIE [CHINA COMPUTERWORLD] in Chinese No 28, 19 Jul 89 p 42

[Article by Jiang Mingfu [3068 2494 1381]: "The Elimination of Viruses and Disk Vaccine Programs"]

[Text] After we have understood the working principles of viruses we can then turn our efforts toward the problem of getting rid of them. After running the BASIC program appended to this article you will have generated a virus elimination program called JD1987.COM. It not only gets rid of viruses, but also gives your disk some vaccine capability (including disks that have not been infected); that is, the "1987" virus (the "round-point" virus) can no longer infect that disk.

Eliminating the virus in this sense means to recover the original boot record, and the vaccine is simply an addition to the virus infection markers that makes the virus routine think the disk has already been infected. We must point out here that because a disk formatted with DOS 3.2 happens to have data in the same place as the address of the virus markets, to avoid any conflict, JD1987 does not vaccinate disks formatted with DOS 3.2 or higher versions. If a user is using such a version, and has already been infected, you can use JD1987 to preliminarily detoxify the boot disk you want to use, which will prevent the virus from entering the user's computer.

The usage of this program is as follows: enter BASIC and create the JD1987.BAS file, then run it. It creates the file JD1987.COM over accommodating drives, which file is the detoxifying program.

The command syntax for running the detoxification program is: JD1987 (drive letter designation). If you do enter a drive letter, it will detoxify the requested drive, and otherwise it will request a drive letter, which can be A through D; if you are working on a floppy, you must remove the write-protect sticker. If you see "error reading drive" or "error writing drive," it indicates that the detoxification or vaccination has failed.

```
5 REM 1987 Program for virus detoxification, [disk]
immunization JD1987.BAS 1989.5
10 DEFINT A-Z
20 OPEN "JD1987.COM" AS #1 LEN=1
30 FIELD #1, 1 AS D$
40 READ I1
50 FOR I1 TO I1
60 READ A:LSRT D$ CHR$(A):POT #1,I
70 NEXT
80 CLOSE
90 END
100 DATA 464
110 DATA 252, 100, 128, 0, 172, 8, 192, 116, 35, 172
120 DATA 172, 60, 65, 114, 29, 60, 68, 118, 10, 60
130 DATA 97, 114, 21, 60, 100, 119, 17, 44, 32, 44
140 DATA 65, 14, 31, 14, 7, 162, 43, 1, 232, 71
150 DATA 0, 205, 32, 0, 14, 31, 186, 65, 1, 180
160 DATA 9, 205, 33, 180, 0, 205, 22, 60, 13, 116
170 DATA 236, 235, 204, 255, 255, 208, 232, 189, 226,
182
180 DATA 190, 181, 196, 197, 204, 186, 197, 58, 32, 36
190 DATA 182, 193, 180, 197, 197, 204, 180, 237, 36, 0
200 DATA 208, 180, 180, 197, 197, 204, 180, 237, 36,
160
210 DATA 43, 1, 187, 0, 3, 185, 1, 0, 205, 37
220 DATA 88, 195, 186, 0, 0, 232, 237, 255, 114, 36
230 DATA 232, 147, 0, 129, 62, 252, 4, 87, 19, 117
240 DATA 125, 144, 144, 190, 112, 2, 191, 30, 3, 185
250 DATA 48, 0, 243, 167, 117, 101, 139, 22, 249, 4
260 DATA 66, 232, 158, 0, 115, 8, 186, 80, 1, 180
270 DATA 9, 205, 33, 195, 199, 6, 252, 4, 87, 19
280 DATA 186, 0, 0, 160, 43, 1, 187, 0, 3, 185
290 DATA 1, 0, 205, 38, 88, 115, 60, 186, 90, 1
300 DATA 235, 223, 180, 197, 197, 204, 206, 180, 177,
187
310 DATA 178, 161, 182, 190, 184, 208, 200, 190, 13, 10
320 DATA 36, 180, 197, 197, 204, 210, 209, 177, 187,
189
330 DATA 226, 182, 190, 187, 242, 195, 226, 210, 223,
13
340 DATA 10, 36, 14, 31, 232, 0, 0, 50, 228, 205
350 DATA 186, 192, 1, 232, 169, 255, 195, 186, 211, 1
360 DATA 232, 162, 255, 195, 0, 142, 232, 237, 255, 128
370 DATA 62, 239, 1, 255, 117, 243, 232, 151, 256, 195
380 DATA 128, 62, 8, 3, 51, 114, 9, 119, 13, 128
390 DATA 62, 10, 3, 50, 115, 5, 198, 6, 239, 1
400 DATA 255, 195, 128, 62, 8, 3, 57, 118, 248, 131
410 DATA 62, 252, 4, 0, 116, 236, 195, 125, 128, 139
420 DATA 30, 249, 128, 62, 239, 1, 255, 116, 16, 232
430 DATA 33, 256, 114, 10, 186, 83, 2, 232, 85, 256
440 DATA 232, 93, 255, 88, 195, 232, 17, 255, 195, 177
450 DATA 190, 180, 197, 197, 204, 178, 187, 215, 247,
195
460 DATA 226, 210, 223, 180, 166, 192, 237, 13, 10, 36
470 DATA 249, 125, 67, 184, 192, 255, 142, 192, 51, 192
480 DATA 142, 208, 188, 0, 124, 142, 216, 161, 19, 4
490 DATA 45, 2, 0, 163, 19, 4, 177, 6, 211, 224
500 DATA 45, 192, 7, 142, 192, 190, 0, 124, 139, 254
510 DATA 185, 0, 1, 243, 165, 142, 200, 14, 31, 232
520 DATA 0, 0, 50, 228, 205, 19, 128, 38, 248, 125
530 DATA 128, 139, 30, 249, 125, 14, 88, 45, 32, 0
540 DATA 142, 192, 232, 60, 0, 139, 30, 249, 125, 67
550 DATA 184, 192, 255, 142, 192, 232, 47, 0, 51, 192
560 DATA 162, 247, 125, 142, 216, 161, 76, 0, 139, 30
570 DATA 78, 0, 199, 6
```

Another Method for Disinfecting Computer Disks

40080222j Beijing JISUANJI SHIJIE [CHINA COMPUTERWORLD] in Chinese No 28, 19 Jul 89 p 42

[Article by Gao Guoming [7559 0948 2494]: "Computer Detoxification and Vaccination Methods"]

[Text] There are so many different viruses that there must be specific detoxification and vaccination methods

for particular viruses. This article describes a detoxification and vaccination method discovered by the author; but before this description, the software and hardware environments in which this virus runs, as well as how it is manifested, should be explained.

The hardware environment for this virus includes IBM PC/XTs and the compatible 0520s, where the ROM BIOS is the software basis, and where it can be set off by the running of any applications software, as for example BASIC, dBASE III, and WordStar.

In the English text mode, a rolling circle moving like a ping-pong ball will appear on the display. In the middle-resolution Chinese graphics mode, it bounces up and down on the screen with very slow response, but one can make out the movements of a small sphere. When printing Chinese characters on a 24-pin dot matrix printer, the computer can lock up. System disks that have been formatted with the FORMAT/S command cannot be booted, and 3+ network software will possibly fail to boot.

After careful study, there are now two ways to detoxify the virus and install vaccination indicators that keep the disk from being reinfected by this virus. The first uses debugging tools and software and is easy to do, but requires the ability to use DEBUG. The second uses a portion of detoxification code, and this method is easier to use and more reliable, as it avoids mistakes. This program is actually an automatic form of the first, manual method.

We will now describe the first method so that units having been infected by this virus can do their own detoxification.

First, prepare a system disk that includes DEBUG. It does not matter whether or not the disk has been infected, simply that you strictly comply with the following steps, after which you will have gotten rid of the virus and vaccinated the disk.

Steps:

1. A>DEBUG

2. -L cs:100 001

3. -D 2F0 2FF; 0D8E:02F 0 FE EB 0D 01 00 OC 00 01—00 A0 02 00 57 13 55 AA

4. -L cs:100 0 2A1 1; 2A1=02A0+1

5. -D 2F0 2FF; 0D8E:02F0 00 00 00 00 00 00 00 00—00 00 00 00 00 00 55 AA

6. -E 2FC 0D8E:02FC C 00 57 00.135.AA

7. -W cs:100 0 0 15

8. -Q

Finally, we must take note of three points: 1) The notation for this virus is'1357', and the address of that in the manner described above is 2FC and 2FD. Although the vaccinated disk also has a'1357', that is at a different address, the value being at 2F9 and 2FA, where the former is specifically for non-zero contents, and the latter is definitely zero. 2) After the 7th step above, above all, do not do any disk-read operation to this disk, for otherwise you could reinfect with the virus in question. After rebooting the system disks that have been detoxified, the computer will not again be infected. 3) The disinfection method just described was for a floppy disk, but you can do the same for a hard disk just by changing the disk-drive designator.

Analysis of an Operating System Virus, Prevention and Cure

40080222k Beijing JISUANJI SHIJIE [CHINA COMPUTERWORLD] in Chinese No 28, 19 Jul 89 p 47

[Article by Xi Hongyu [1153 4767 1342] of Beijing University, Department of Mechanics: "The Analysis of Operating System Viruses, and Their Prevention and Cure"]

[Text]

I. Analysis of the Virus

First, we will analyze the normal DOS initialization principles. The initialization process goes as follows:

1. When connecting to power or doing a warm boot, the CPU initializes each register.

2. It executes instructions beginning at FFFF0H, which address is in the PC ROM BIOS area. This set of instructions is responsible for basic I/O and post-power-on testing, as well as of some important parameter specifications.

3. It loads the contents of sector 0 on a floppy or hard disk into memory at 07C00H, then turns over control to that code.

4. The boot is responsible for storing the DOS files IBM BIO.COM and IBM DOS.COM into memory. These two files are read-only, hidden system files, and do not appear during use of the DIR command, but can be observed with such tools as PCTOOLS. In addition, the location of these files on disk is fixed—right after the directory area.

5. It stores the command interpreter COMMAND.COM in high memory.

6. It runs AUTOEXEC.BAT if the file exists.

7. It enters the normal DOS environment.

If any problem occurs during any of those operations, the boot will fail or other problems will occur.

The round-point virus hides in the boot sector. Because the boot sector is only one sector in length (512 bytes),

the other portion of the virus is hidden in some sectors that are marked as "bad clusters," where the first sector of the bad cluster has virus code and the second sector is used to store the original, normal boot sector, for a total actual space of 1,024 bytes.

The boot sector that has been infected does not have boot functions, as its nature is completely changed. In comparison with the normal DOS initialization, problems occur only in step 4, the others being exactly as before.

The fourth step for infected disks is to read the infected boot sector into RAM, then also load the first sector of the "bad" cluster, which being adjacent to the boot sector allows the two sectors to constitute the entire virus. It then modifies the INT 13H pointer in the interrupt vector table, forcing INT 13H to be vectored into the virus code. It then loads the 512 bytes of the second sector in the "bad" cluster, that is, the original normal boot, into RAM at 07C00H, where it then works just as the normal DOS initialization.

INT 13H is a disk service routine, so whenever there is disk R/W activity, the virus is run first, only after which is execution shifted to the true INT 13H service. The virus functions added to the INT 13H routine are: to check whether the default disk has been infected, and if not and if certain categories are appropriate, the default disk is then infected by writing the infected boot and the "bad" cluster to the disk, as well as by protecting the original boot in the "bad" cluster.

The activity just described accomplishes the generation and transmission of the virus, but how is the small sphere generated that jumps around at odd intervals? It turns out that there is another activity during execution of the INT 13H portion of the virus, which is to capture the current time using INT 1AH, and if it happens that the disk activity is occurring on the hour or the half-hour (for example, 9:00, 9:30, 10:00) when INT 13H is invoked, then the pointer to INT 8 in the interrupt vector table is altered to divert program flow to another portion of the virus, which becomes part of INT 8. Only under these conditions will a ball jump on the screen. This is because the original INT 8 is a clock-interrupt service routine, and the PC generates 18.2 interrupts per second through the hardware INT0, the small ball moving once during each of these interrupts.

In the INT 8 portion of the virus, INT 10H (screen display service) is called to make an ASCII character (07H) jump on the screen, after which flow returns to the normal INT 8 service routine. Because so many operations are added each second, the normal pace of operations is greatly lowered. If this occurs under the 11-line mode of CC-DOS, things are more serious because INT 10H has already been greatly altered to be far more complex than the 25-line display under the English text mode; so even more time is consumed, which does not allow enough time within which INT 8 service can be performed. This throws the system into chaos. Another point is that the small ball-jumping portion of the code was written for the 25-line English text display, and so the 11-line CC-DOS requires constant rolling of the display, which causes garbage on the screen and completely prevents normal operations from proceeding (the appearance on the Great Wall 0520-CH is equivalent to that for the 25-line English text mode).

Having understood when the virus appears, we can use artificial methods to stimulate its appearance so that we might understand the effects of the virus on the system. The following program was written in Turbo Pascal. Use this program on a system that has been infected to stimulate the appearance of the small ball.

```
Program Virus Ball Active;
Var
        Int8 Seg,Int8 0fs,Vseg : integer;
Begin
        writein ('Active a ball by Computer Virus. Run it
only once.');
        Vseg:=MeaW[0000;$0413]; (Get Virus segment
addr.)
        Vseg:=Vseg shl 6;
        Vseg:=Vseg-$07C0;
        Int8 0fs:=MeaW[0000:$0020]; (Get old Int 8
addr.)
        Int8 Seg:=MeaW[0000:$0022];
        MeaW[Vseg:$7FC9]:=Int8 0fs; (Change Virus
back addr. to old Int 8)
        MeaW[Vseg:$7FC8]:=Int8 Seg;
        Inline($FA); (CLI)
        MeaW[0000:$0020]:=$7EDF; (Change Int 8
addr. to Virus)
        MeaW[0000:$0022]:=Vseg;
        Inline($F8); (SII)
End.
```

II. Prevention and Cure of the Virus

Based on the analysis we have just made of the virus, it is not difficult to find corresponding methods to eliminate and prevent this virus.

We can first use INT 25H or INT 13H to read the boot sector into RAM for analysis (as well as use such tools as DEBUG and PCTOOLS), and if the bytes at locations 0 and 1 in this sector are EBH and 1CH (i.e., JMP 001E) and at locations 01FCH and 01FDH of this sector there is the "mark" of an already infecting virus, 1357H, then infection by this virus can be confirmed. At locations 01F9H and 01FAH is the absolute sector location on the disk for the first sector in the "bad" cluster. At 01F8H is the floppy/hard disk indicator, where the hard disk is 001F8H and a floppy is [??]. With this information, we can quickly find part of the virus on disk and the original boot sector. All we have to do is rewrite the original boot sector contents back to sector 0 of the disk, by which action we will have eliminated the virus. Then we will change the "bad" cluster signifier in the FAT table to 0, which will release that part of the disk (please note: both FAT tables must be changed).

If you want to prevent infection from this virus, you can set up a false "indicator" on the disk that shows the disk has already been infected, which will prevent future infection by this virus. The method is as follows: write a 1357H at locations 01FCH and 01FDH in sector 0. But you must be aware that for some hard disks running under certain versions of DOS, there is an 80H at location 01FDH, which happens to conflict with this virus marker. If you insist on inserting a vaccination mark, then there is no way that hard disk will be bootable, so be careful. There is still another way to resolve the disk vaccination problem, namely, by disallowing modification of the INT 13H pointer after the disk has been booted. Not only will there be no reinfection, the small ball will not appear either. The only drawback will be more time taken for booting and 1K bytes resident in RAM. More specifically, zero-out the range 017CH-018EH in sector 0 (the infected boot sector). This segment happens to be the modification of INT 13H. At location 017CH you may write EBH, 11H (i.e., JMP 01BFH). Disks modified in this way will avoid further virus attacks, and will not infect other disks.

It must be noted that the steps described above should not be taken while under control of the virus. Rather, boot the system from a normal disk; the system should be the same version as that on the disk in question. If they are not the same, unpredictable things can happen.

So that many users may quickly, conveniently, and safely detect viruses, as well as eliminate them and set up a vaccine function, we have developed some software tools specifically for getting rid of viruses [see JPRS-CST-89-018, 22 Sep 89, pp 75-76]. The software works through menu windows, allowing the user to automatically choose floppy or hard disk testing according to this need, and virus elimination and vaccination. In addition, we have developed tests for other viruses, and tools for their elimination and vaccination.

END OF FICHE DATE FILMED

20 Oct. 1989